EMD Techniques of Image Steganography

A Comparative Study

Mamta Kalra, Parvinder Singh
Department of Computer Science & Engineering
Deenbandhu Chhoturam University of Science & Technology

***Abstract*— Exploiting Modification Direction (EMD) is a technique to hide secret data into digital images. This paper reviews different EMD techniques to hide the confidential data. The main idea of EMD is to embed secret data into digital image in such a way that it provides high embedding efficiency as compared to the other techniques. The brief introduction of various EMD schemes and their comparisons are presented in this paper.**

Keywords- Steganography, Exploiting Modification Direction (EMD), Stego image.

I. INTRODUCTION

Since the rise of internet secure data transmission has been a significant problem. The early approach was to secure communications is via data encryption. In data encryption, the content of the message is kept secret whereas sometimes the existence of message is also need to be kept secret. The technique used to implement this is called steganography. Steganography is a technique for hiding secret message into some other medium in such a way that no one can detect the existence of the hidden message. The word steganography is basically derived from two Greek words [1]: Steganos and Graphie, which means covered writing. Therefore steganography is a technique of hiding secret and confidential message in another media such that no one apart from the intended recipient can even detect the presence of the hidden message.

The main goal of the steganography is to hide messages inside other messages in such a way that it does not allow any eavesdroppers and attacker to even detect that there is a second secret message present inside that message [2-12].

One way for improving security of the Steganographic system is to reduce the amount of changes introduced in the cover object due to embedding secret data i.e. increasing the embedding efficiency of the Steganographic system. Various techniques were designed for this purpose. EMD(Exploiting Modification direction) is one those Steganographic techniques that leads to higher embedding efficiency as compared to other techniques such as run length encoding [13] and matrix encoding [14].

EMD is a method of steganography embedding in digital images in which each secret digit in (2n+1)-ary notational system is carried by n cover pixels and only one cover pixel is either increased by one or decreased by one or remain same. In general, for each group of n cover pixels there are 2n possible ways of alteration. These 2n ways of modification and one case in which no pixel is changed form (2n + 1) different values of a secret digit. The direction of modification of cover pixel is fully exploited that's why it achieves high embedding efficiency as compared to other techniques.

Various modifications of EMD are also designed which are given in this paper. The rest of the paper is organized as follows: In section II, concepts of EMD scheme has been explained. Various EMD techniques have been explained and compared in section III. In section IV, the complete paper is concluded.

II. EXPLOITING MODIFICATION DIRECTION TECHNIQUE

Zhang et al [15] proposed a data hiding method that exploits the modification directions called EMD technique that is used to convert binary secret data into secret digits(d) in (2n+1)-ary notational system such that n pixels can be used to carry one secret digit. In this technique, secret message is firstly converted into secret digits in (2n+1)-ary notational system and then each secret digit are embedded into pixel group ($g_1,g_2,\ldots\ldots,g_n$). To embed secret digit d, value of extraction function f_e is calculated by using (1).

$$f_e(g_1, g_2, .., g_n) = (g_1 \times 1 + g_2 \times 2 + \cdots + g_n \times n \bmod (2n+1) \quad (1)$$

If the value of f_e is not equal to the secret digit d, only one of the pixels from the pixel group has to be incremented or decremented by one. If both the values are same, then there is no need to change any pixel. And the process is repeated until no secret digit is left.

In the extraction procedure, same equation is used for each pixel group ($g_1,g_2,\ldots\ldots,g_n$) to find out the secret digits and then all the secret digits are converted back into binary notation from (2n+1)-ary notation to find out the secret message.

Fig.1. shows the extraction function matrix for simplest case of n=2, where each square is labeled with its extraction value f_e and the f_e value of each square and its 2n neighbors are mutually different. After that each secret digit will be mapped to a group. If the value of secret digit d and extraction value f_e are same then no change is required in the group. But both are not same, value of r is calculated using (2). If $r \leq n$, then g_r is increased by 1; otherwise g_{2n+1-r} is decreased by 1.

$$\boldsymbol{r = (f_e - d) mod\ (2n + 1)} \qquad (2)$$

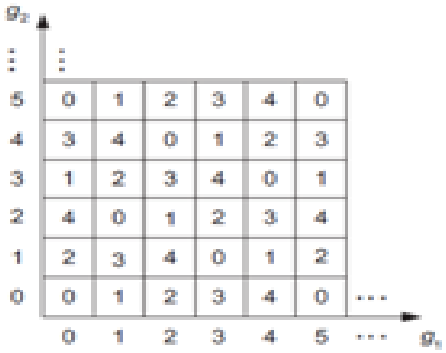

Figure 1. Extraction Function for n=2

III. VARIOUS IMPROVEMENTS OF EMD SCHEME

The technique proposed by Zhang et al [15] shows high embedding efficiency. Also the PSNR value is above fifty. But it store only one secret digit in each n-pixel group. So to improve the embedding capacity, various improved EMD schemes were proposed. Some of which are explained below:

A. *Improved Exploiting Modification Direction(IEMD) technique:*

Lee et al [16] proposed a new scheme that is an improvement over EMD technique. This new approach achieves 1.5 times embedding capacity compared with the EMD technique without losing stego image quality and security. In this scheme, secret message is converted into secret digits (d) in 8-ary notational system. And each digit is stored in 2 cover pixels. The extraction function proposed in[12] is

$$f_e(X, Y) = (X \times 1 + Y \times 3) mod\ 8 \qquad (3)$$

where X and Y represent the grayscale value of two cover pixels in pixel-group.

For each secret digit d, value of f_e is calculated. If d=f_e, then no changes in the pixel values are required. If values are different, then either X or Y or both are needed to be changed. The changes are either +1 or -1 only. After embedding all the secret digits, stego image are transmitted to receiver and the same extraction function is applied to the pixel pairs of the stego image to retrieve the secret digits. After extracting all the digits, they are converted back into binary notation to retrieve the secret message.

B. *Improved data hiding method by EMD:*

EMD scheme was further enhanced by Byun et al in [17]. In this, author proposed a new EMD scheme in which data can be embedded in each pixel of the cover image which enhances the embedding capacity further as compared with the previous technique. In this approach, secret data is converted into secret digits in (2n+1)-ary notational system and each secret digit d are carried by one cover pixel. In this embedding method, embedding function is

$$f = p_i + x\big(mod(2n + 1)\big) \qquad (4)$$

where p_i is the pixel value.

Then, value of f is calculated by (4), where $|x| \leq n$. And a new pixel value $\boldsymbol{p_i'}$ is obtained by (5)

$$p_i' = p_i + x \qquad (5)$$

Where x is selected to satisfy f=d condition.

In the extracting method, the extraction function is

$$d = p_i'(mod(2n + 1)) \qquad (6)$$

Using (6), the value of secret digit d is obtained. And after obtaining all the secret digit sequence, they are converted back into binary sequence to obtain the secret message.

C. *EMD scheme on Wet image:*

In 2009, Chang et al [18] introduced a new data hiding technique that is basically a combination of two techniques. These two techniques are

- Wet Paper Coding
- Fully Exploiting Modification(FEM) Method

In Wet paper coding [19], all the cover pixels are divided into two categories: Wet pixels and Dry pixels. The wet and dry pixels can be chosen randomly or based on a pre-determined policy. Then the secret message is embedded only in the dry pixels of the cover image. In FEM method [20], secret message is embedded into cover image by slightly modifying the direction of the original cover image from the stego image.

This technique has three phases:

- Pre-processing phase
- Embedding phase
- Extraction phase

During pre-processing phase, all the cover image pixels are defined as either dry or wet pixels based on a shared key between the sender and the receiver.

Then in embedding phase, each pair of cover image is taken as a token for embedding secret digit using FEM method. Three types of tokens (pixel pairs) can be generated.

- Restricted pairs of wet pixels (RPW)
- Non-restricted pairs of wet pixels (NRPW)
- Pairs of dry pixels (DP)

If the token is RPW than it is non-embeddable (no data can be stored in that), otherwise it is embeddable. Before embedding, secret data is expressed into secret digits with $\boldsymbol{n^2}$-notational system and value of s is calculated for each pixel pair by using (7)

$$s = f(p_i, p_j) = \big((n-1) \times p_i + n \times p_j\big)\ mod\ n^2 \qquad (7)$$

If the pixel pair is classified into DP category, then first pixel is taken as $\boldsymbol{p_i}$ and second pixel is taken as $\boldsymbol{p_j}$. If the pixel pair is from NRWP category, then the dry pixel is mapped to $\boldsymbol{p_i}$ and wet pixel is mapped to $\boldsymbol{p_j}$. To embed the secret digit d into embeddable pair, $\boldsymbol{p_i}$ value is changed with smallest distortion such that d=s condition holds.

In the extraction phase, when the receiver receives the stego image, he or she uses the same secret key to identify the wet and dry pixels and divide the complete stego image into pixels pairs. From the embeddable pairs, receiver extracts the secret

digits by using (7) and converted back to binary notation to obtain the secret message.

D. General improving EMD scheme:

In EMD [15] and IEMD [16], hiding technique is fixed and extraction formula needs to be kept secret in order to enhance the security because once the formula leaked to the public, anyone can easily extract the hidden message. To deal with this problem, W.C.Kuo et al [21] proposed two new EMD schemes to improve the safety problems of EMD [5] and IEMD [16].

- The improved version of high capacity EMD hiding technique
- The generalized high capacity EMD data hiding techniques

In both the techniques, general extraction formula that will be used is given by (8).

$$f_e(X,Y) = (X \times a + Y \times b) mod\ 8 \qquad (8)$$

Where a and b are weighting values and have to satisfy a≠b and (a+b) mod 8≠0.

Based on a set of a, b, all (a, b) pairs are created that satisfies the above two conditions. And a seed value is used to decide which (a, b) is used as a weighting values parameter for the extraction function and value of extraction function is calculated by using (8).

The improved version of high capacity EMD hiding technique:

In this technique, table checking approach is used in order to change the value of weighting parameters. After deciding weighting parameters based on seed value, we uses the random weighting value to check upon the modulo table to determine which way we should use to change the pixel pair (X,Y) in the cover image. Then we calculate the value of f_e using (8) and find out the difference between f_e and secret digit s using (9).

$$d = (f_e - s) mod\ 8 \qquad (9)$$

After getting the difference d, we check the table values in order to see which pixel pair have that difference value d and replace our pixel pair(X,Y) with (X',Y') and then transmit both stego image and tables to the receiver.

The generalized high capacity EMD data hiding techniques

In this technique, there is no need to predetermine the entire table values for all (a, b) pairs. Instead rather than using table checking approach, a generalized approach is used in order to improves the security issues of EMD [15] and IEMD [16]. Using this approach, we can speed up the data embedding process without any extra table storage. In this approach, with each seed value, a pair (a, b) and values of α and β are associated. When we calculate the value of extraction function f_e and then difference between f_e and secret digit s using (9), meanwhile we also apply α and β into the generalized equation to get the results as shown in fig. 2 and 3.

TABLE I. THE CHANGING OF X, Y FOR SEED VALUE (0-3)

X-α, Y+β	X,Y+ β	X+α, Y+ β
X-α, Y	X,Y	X+α, Y
	X,Y- β	X+α, Y- β

TABLE II. THE CHANGING OF X, Y FOR SEED VALUE (4-7)

X-α, Y+β	X,Y+ β	X+α, Y+ β
X-α, Y	X,Y	X+α, Y
	X,Y- β	X+α, Y- β

Therefore without wasting extra space for table storage we can easily find out the desired pixel value (X, Y) and embed all secret digits into cover image and form a stego image.

Using these approaches, improvements over safety issues can be achieved even the extraction function is announced to the public.

E. Generalized EMD:

In all the previous schemes, the secret message is first converted into some special base notational system whereas the scheme explained in [22] doesn't require any need to convert message into some other format; instead the message is directly embedded into cover message in binary format using EMD approach. This method is based on general improved EMD technique and named as generalized EMD method. In this method, (n+1) bits binary message is carried by n adjacent pixels and each pixel can be either increased by 1 or decreased by 1 or remain same. The extraction function used in [10] is:

$$f_e(g_1, g_2, .., g_n) = \left[\sum_{i=1}^{n} \left(g_i.(2^i - 1)\right)\right] mod 2^{n+1} \qquad (10)$$

F. EMD based image steganography scheme in spatial domain:

Hajizadeh et al [23] proposed an extended form of EMD scheme in which eight modification directions are used to embed secret message into cover pixel pair instead of 5 modification directions. The modified extraction function used in this scheme is defined as:

$$f = f(x_i, x_{i+1}) = \left((m-1) \times x_i + \times x_{i+1}\right) mod\ m^2 \qquad (11)$$

where $m \geq 2$.

In this scheme, k ($=\lfloor \log_2 m^2 \rfloor$) bits secret message are embedded into a block of 2 cover pixel (x_i, x_{i+1}) by increasing or decreasing x_i or/and x_{i+1} at most by r ($=\lfloor m/2 \rfloor$ known as searching radius) or remaining same to attain the stego pixel pair.

In order to achieve high security, two steps of image blocking are used in this technique and in each step; image is divided into further sub-images. And a random number, generated by a pseudo random number generator using secret key, is used to select the random sub–images for embedding data. In this way, the data is hidden in different parts of the image and the intended recipient that knows the secret key will be able to extract the hidden message.

A new parameter, known as Data Pattern Modifier (DPM) which is a positive integer lies between 0 to (2^n-1) is defined in this scheme. Once the value of this parameter is initialized, it is converted into k bit binary sequence and is used to define 2 new parameters i.e. XORP (XOR Pattern) and XNORP (XNOR Pattern).

During embedding, k bits of secret message are first converted into decimal number d and value of extraction function f is calculated using (11). If both values are same then no changes are required in pixel values. If values are not same then a new pair value is selected from searching area defined via $W_{(2\times r+1,\ 2\times r+1)}(m, (x_i, x_{i+1}), r)$ having f value same as d. But the selected pair may not provide optimal solution with minimum distortion therefore other pairs are also searched from the searching area W with center as the selected pair and the pair having minimum distortion will be selected and the final stego image pair will be modified with that value. This process is repeated until the entire message is not embedded into the cover image.

At the receiver side, the specified embedding pattern for each block is needed to extract the secret message. For this purpose, a 2 bit binary key is assigned to each embedding block by the sender.

Therefore the intended recipient having that secret pattern, will only be able to extract message from the stego image.

G. *Optimized EMD:*

In 2010, Lin et al [24] proposed optimize EMD technique that is based on the relationship between n and payload value. In EMD scheme, a group of n pixels are used to embed a secret digit in (2n+1)-ary notational system. The value of n has to be selected carefully because it will decide the amount of pixel group and payload for that group. If the value is selected too large, then it will not provide the enough space to embed the entire secret message whereas if the value is too small, then it will use more numbers of pixels to embed data more than it actually required. So Lin et al in [22] analyze the relationship between payload and n which is defined by (12).

$$\left\lfloor \frac{I_s}{n} \right\rfloor \times \lceil \log_2(2n+1) \rceil \geq p \qquad (12)$$

Where I_s means the total number of pixels in the cover image, n means total number of pixels in a group and p means length of the payload. Since both p and I_s are known, hence the maximum value of n can be calculated easily which provides the optimal solution.

TABLE III. SUMMARY OF VARIOUS EMD TECHNIQUES

Researcher	Year	Advantages	Disadvantages
Zhang et al [15]	2006	• Embedding efficiency and embedding rate are more than run length encoding and matrix encoding. • Stego image quality is also good.	• Less efficient. • Safety issues are there. • Message needs to be converted into another format hence more time is required for embedding. • Embedding capacity is limited.
Lee et al [16]	2007	• Embedding capacity is more than basic EMD. • Embedding rate is 1.5 times as compared to basic EMD.	• Safety issues are there. • More time for embedding.
Byun et al [17]	2008	• Embedding capacity is 2 times as compared to basic EMD. • Stego image quality is also good.	• Due to high embedding capacity PSNR value decreases. • Safety issues are there.
Kuo et al [22]	2009	• No need of message conversion hence less time for embedding. • Stego image quality is also good. • Embedding capacity is also high.	• Safety issues are there.

Kuo et al [21]	2009	• In improved version of high capacity EMD technique, data embedding strategy is fast. • In generalized high capacity EMD technique, less storage is required. • Both techniques provide high embedding capacity and security.	• In improved version of high capacity EMD technique, more storage is required to store tables. • In generalized high capacity EMD technique, more time is required to embed data.
Chang et al [18]	2009	• Provides high security. • Stego image quality is also good.	• Does not utilize all dry pixels to embed secret data.
Lin et al [24]	2010	• Provides low distortion and high PSNR value.	• Embedding capacity is limited.
Hajizadeh et al [23]	2013	• Provides high security. • Embedding capacity is also high	• Stego image quality is not so good.

IV. CONCLUSION

In this paper, we have discussed different EMD techniques to hide secret data inside the image. EMD techniques provide better embedding efficiency and embedding rate as compared to matrix encoding and run length encoding. EMD technique proposed in [16] improves the 1.5 times embedding capacity as compared to basic EMD which was further improved in [17]. Generalized EMD, IEMD and scheme proposed in [21] provide similar image quality and embedding capacity, but in Generalized EMD scheme there is no need of message conversion hence less time is required for embedding process as compared to IEMD. Among all the EMD schemes, Optimized EMD provides the highest PSNR ratio.

ACKNOWLEDGMENT

The work in this paper is funded by Major UGC Project "Department of a model for secured Communication".

REFERENCES

[1] Rengarajan Amirtharajan, John Bosco Balaguru Rayappan, "An intelligent chaotic embedding approach to enhance stego-image quality", Information Sciences 193, pp. 115–124, journal homepage: www.elsevier.com/locate/ins, 2012.

[2] Parvinder Singh, Sudhir Batra, H R Sharma, "Message Hidden in 6th and 7th Bit", Proceedings of International Conference on Controls, Automation and Communication System, Dec. 22-24, 2004, Allied Publishers, pp-281-284.

[3] Parvinder Singh, Sudhir Batra, HR Sharma, "Evaluating the Performance of Message Hidden in 1st and 2nd Bit Plane", WSEAS Transactions on Information Science and Applications, issue 8, vol 2, August 2005, pp 1220-1227.

[4] Parvinder Singh, Sudhir Batra, HR Sharma, "Message Hidden in 1st and 2nd Bit Plane", Proceedings of 9th WSEAS International Conference on Computers, Athens, Greece, July 14-16, 2005, pp 1-5.

[5] Parvinder Singh, Sudhir Batra, H R Sharma, "Steganographic Methods Based on Digital Logic", 6th International Conference on Signal Processing, Dallas, USA, March 22-24,2007.

[6] Prince Kumar Panjabi, Parvinder Singh, "An Enhanced Data Hiding Approach using Pixel Mapping Method with Optimal Substitution Approach", International Journal of Computer Applications, vol.74(10), July 2013, pp. 36-43.

[7] Parvinder Singh, Sudhir Batra, HR Sharma, "Hiding Credentials in Biological Images", A & B Research, vol 22(1), Jan 2006, ISSN 0970-1970, pp 22-25.

[8] Sonam Chhikara, Parvinder Singh, "SBHCS: Spike based Histogram Comparison Steganalysis Technique", International Journal of Computer Applications, vol.75, 2013.

[9] Sudhir Batra, Parvinder Singh, "A Class of $ q $-ary 2-IPP Codes", Journal of Informatics and Mathematical Sciences 5 (2), 65-76.

[10] Parvinder Singh, Sudhir Batra, HR Sharma, "A review of digital signatures and status in India", WSEAS Transactions on Computers 4 (4), 408-410.

[11] Jasvinder Kaur, Manoj Duhan, Ashok Kumar, "Digital Logic Embedding Using Single Row." International Journal on Computer Science & Engineering, vol. 3, no. 12 , 2011.

[12] Currie, D.L. & Irvine, C.E., "Surmounting the effects of lossy compression on Steganography", 19th National Information Systems Security Conference, 1996.

[13] X. Zhang and S. Wang, "Dynamically running coding in digital steganography," IEEE Signal Processing Lett., vol. 13, no.3, pp. 165-168, Mar. 2006.

[14] A. Westfeld, "F5: a steganographic algorithm," in Proc. 4th Int. Workshop Information Hiding, Lecture Notes in Computer Science, vol. 2137, pp. 289-302, 2001.

[15] X. Zhang and S. Wang, "Efficient Steganographic Embedding by Exploiting Modification Direction," IEEE Communications Letters, vol. 10, no. 11, pp. 781-783, November 2006.

[16] Chin-Feng Lee, Yi-Ren Wang and Chin-Chen Chang, "A steganography method with high capacity by improving Exploiting Modification Direction" IIHMSP, Volume 1, pp.497 – 500, 2007.

[17] Jin-Yong Byun, Ki-Hyun Jung and Kee-Young Yoo, "Improved Data Hiding Method by Exploiting Modification Direction", International Symposium on Ubiquitous Multimedia Computing, pp. 264–266, 2008.

[18] Chin-Chen Chang, Zhi-Hui Wang, Yi-Hui Chen and Ming-Chu Li, "A Wet Image Data Hiding Scheme Based on Coordinate Modifications" Third International Symposium on Intelligent Information Technology Application, 2009.

[19] Fridrich, J., Goljan, M., Lisonek, P. and Soukal, D., "Writing on wet paper," IEEE Transactions on Signal Processing, vol. 53, no. 10, pp. 3923-3935, 2005.

[20] Duc, K., Chang, C. C., "A steganographic scheme by fully exploiting modification directions," Technique Report of Feng-Chia University.

[21] C. N. Shyi, S. H. Kuo and W. C. Kuo, "Data Hiding Method Based on High Embedding Capacity by Improving Exploiting Modification Direction" 2008 Conference on Global Logistic Management and Industry Practice Research. 25, pp.455-462, December 2008.

[22] Wen-Chung, Kuo Jiin-Chiou Cheng, Chun-Cheng Wang, "More Efficient Steganoraphic Embedding and Capacity-Improvement by Generalized Exploiting Modification Direction Method" Fourth

International Conference on Innovative Computing, Information and Control, 2009.

[23] Hamzeh Hajizadeh, Ahmad Ayatollahi and Sattar Mirzakuchaki, "A New High Capacity and EMD-based Image Steganography Scheme in Spatial Domain", 2013.

[24] Kai Yung Lin, Wien Hong, Jeanne Chen, Tung Shou Chen, Wen Chin Chiang, "Data Hiding by Exploiting Modification Direction Technique Using Optimal Pixel Grouping" 2nd International Conference on Education Technology and Computer (ICETC),2010.